UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/576,598	05/22/2000	Solomon W. Golomb	06666-032001	1702

20985 7590 06/02/2005

FISH & RICHARDSON, PC
12390 EL CAMINO REAL
SAN DIEGO, CA 92130-2081

EXAMINER	
ORTIZ, BELIX M	

ART UNIT	PAPER NUMBER
2164	

DATE MAILED: 06/02/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/576,598	GOLOMB ET AL.	
	Examiner	Art Unit	
	Belix M. Ortiz	2164	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *15 March 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,3-16,19,21-26,29 and 31-33* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,3-16,19,21-26,29 and 31-33* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

SAM RIMELL
PRIMARY EXAMINER

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Remarks

1. In response to communications files on 15-March-2005, claims 2, 17-18, 20, 27-28, 30, and 34 are cancelled and the specification of the disclosure are amended per applicant's request. Therefore, claims 1, 3-16, 19, 21-26, 29, and 31-33 are presently pending in the application.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1, 3-6, 9, 11, 19, 21-22, 29, and 31-32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Seheidt et al. (U.S. patent 5,787,173) in view of Masters (U.S. patent 5,812,072).

As to claim 1, Seheidt et al. teaches a cryptography method (see abstract), comprising:

determining information to be encrypted (see column 1, lines 12-15; column 1, lines 45-51).

Seheidt et al. does not teach encrypting the information using a non-trivial ci-quasigroup to encode the information.

Masters teaches data conversion technique (see abstract), in which he teaches encrypting the information using a non-trivial ci-quasigroup to encode the information (see column 18, lines 15-30; column 22, lines 30-39; column 25, lines 34-36; column 34, lines 4-10; and column 43, lines 48-52).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Seheidt et al., to include encrypting the information using a non-trivial ci-quasigroup to encode the information.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Seheidt et al. by the teaching of Masters, because encrypting the information using a non-trivial ci-quasigroup to encode the information, would enable the cryptography method since the non-trivial ci-quasigroup excludes the use of groups, the quasigroup that are not groups are more efficient and more secure than those based on group. The result of the message would be more difficult to decode by unauthorized receiver.

As to claim 3, Seheidt et al. as modified teaches a method further comprising decoding sing the crossed-inverse function of the ci-quasigroup (see Master, column 3, lines 53-67 and column 4, lines 1-14).

As to claim 4, Seheidt et al. as modified teaches wherein the encrypting comprises carrying out a first encryption to get a first result, then carrying out a second encryption using the first result, and encryption can be iterated an arbitrary number of times (see Seheidt et al., column 9, lines 32-39).

As to claim 5, Seheidt et al. as modified teaches a method further comprising defining a rule indicative of the quasigroup (see Masters, column 3, lines 3-67; column 31, lines 49-54; column 34, lines 4-10; column 37, lines 33-35; and column 43, lines 48-52).

As to claim 6, Seheidt et al. as modified teaches a method further comprising defining a rule indicative of the crossed inverse of the quasigroup (see Masters, column 3, lines 3-67; column 31, lines 49-54; column 34, lines 4-10; column 37, lines 33-35; and column 43, lines 48-52).

As to claim 9, Seheidt et al. as modified teaches a method further comprising distributing information indicative of the quasigroup as a public key, and keeping secret the crossed inverse quasigroup (see Seheidt et al., column 3, lines 4-31).

As to claim 11, Seheidt et al. as modified teaches wherein the first and second encryption form iterative encipherment (see Seheidt et al., column 9, lines 32-39).

As to claim 19, Seheidt et al. teaches a cryptography method, comprising:

determining information to be encrypted (see column 1, lines 12-15; column 1, lines 45-51).

Seheidt et al. does not teach encrypting the information using a crossed-inverse quasigroup.

Masters teaches data conversion technique (see abstract), in which he teaches encrypting the information using a crossed-inverse quasigroup (see column 18, lines 15-30; column 22, lines 30-39; column 25, lines 34-36; column 34, lines 4-10; and column 43, lines 48-52).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Seheidt et al., to include encrypting the information using a crossed-inverse quasigroup.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Seheidt et al. by the teaching of Masters, because encrypting the information using a crossed-inverse quasigroup, would enable the cryptography method to know what information the user wants to be secure or the information that the user does not want to be seen by unauthorized person.

As to claim 21, Seheidt et al. as modified teaches a method further comprising decoding using a crossed inverse of the quasigroup (see Master, column 3, lines 53-67 and column 4, lines 1-14).

As to claim 22, Seheidt et al. as modified teaches wherein the encrypting comprises carrying out a first encryption to get a first result, then carrying out a second encryption using the first result (see Seheidt et al., column 9, lines 32-39).

As to claim 29, Seheidt et al. teaches an apparatus comprising a program stored on a computer readable media including instructions (see column 5, lines 53-56) to:

send the encrypted message (see column 3, lines 35-37).

Seheidt et al. does not teach encrypt a message using information indicative of a crossed-inverse quasigroup representation; and

decrypt the message using information indicative of the same crossed-inverse quasigroup representation.

Masters teaches data conversion technique (see abstract), in which he teaches encrypt a message using information indicative of a crossed-inverse quasigroup representation (see column 18, lines 15-30; column 22, lines 30-39; column 25, lines 34-36; column 34, lines 4-10; and column 43, lines 48-52); and

decrypt the message using information indicative of the same crossed-inverse quasigroup representation (see column 3, lines 53-67 and column 4, lines 1-14).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Seheidt et al., to include encrypt a message using information indicative of a crossed-inverse quasigroup representation; and

decrypt the message using information indicative of the same crossed-inverse quasigroup representation.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Seheidt et al. by the teaching of Masters, because encrypt a message using information indicative of a crossed-inverse quasigroup representation; and

decrypt the message using information indicative of the same crossed-inverse quasigroup representation, would enable the cryptography method since the non-trivial ci-quasigroup excludes the use of groups, the quasigroup that are not groups are more efficient and more secure than those based on group. The result of the message would be more difficult to decode by unauthorized receiver.

As to claim 31, Seheidt et al. as modified teaches wherein the arithmetic is one which is based on a multiplication table which is expressed as a rule (see Masters, figure 5).

As to claim 32, Seheidt et al. as modified teaches an apparatus further comprising adding a random seed to the arithmetic (see Masters, column 11, lines 28-32).

4. Claim 7 is rejected under 35 U.S.C. 103(a) as being unpatentable over Seheidt et al. (U.S. patent 5,787,173) in view of Masters (U.S. patent 5,812,072) as applied in claims 1, 3-6, 9, 11, 19, 21-22, 29, and 31-32 above, and further in view of Schweitzer et al. (U.S. patent 5,850,450).

As to claim 7, Seheidt et al. '173 as modified still does not teach a method further comprising carrying out a second encrypting using the arithmetic, and wherein a result of the second arithmetic is encrypted exponentially more than a result of the first arithmetic.

Schweitzer et al., teaches method and apparatus for encryption key creation (see abstract), in which he teaches a method further comprising carrying out a second encrypting using the arithmetic, and wherein a result of the second arithmetic is encrypted exponentially more than a result of the first arithmetic (see column 5, lines 49-61).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Seheidt et al. '173, as modified to include a method further comprising carrying out a second encrypting using the arithmetic, and wherein a result of the second arithmetic is encrypted exponentially more than a result of the first arithmetic.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Seheidt et al. '173 as modified by the teaching of Schweitzer et al., because a method further comprising carrying out a second encrypting using the arithmetic, and wherein a result of the second arithmetic is encrypted exponentially more than a result of the first arithmetic, would enable the cryptography method since exponentiation calculation, according to other characteristics and advantages, speed up the time required for performing a encryption.

5. Claims 8 and 14-16 are rejected under 35 U.S.C.103 (a) as being unpatentable over Seheidt et al. (U.S. patent 5,787,173) in view of Masters (U.S. patent 5,812,072) as applied in claims 1, 3-6, 9, 11, 19, 21-22, 29, and 31-32 above, and further in view of in view of Scheidt et al. (U.S. patent 6,266,417).

As to claim 8, Seheidt et al. '173 as modified still does not teach wherein the encrypting comprises using a non trivial a non-group crossed inverse quasigroup to encode.

Scheidt et al. '417, teaches cryptographic communication process and apparatus (see abstract), in which he teaches wherein the encrypting comprises using a non trivial a non-group crossed inverse quasigroup to encode (see column 2, lines 46-53).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Seheidt et al. '173, as modified to include wherein the encrypting comprises using a non trivial a non-group crossed inverse quasigroup to encode.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Seheidt et al. '173 as modified, by the teaching of Scheidt et al. '417, because wherein the encrypting comprises using a non trivial a non-group crossed inverse quasigroup to encode, would enable the cryptography method since the non-trivial ci-quasigroup excludes the use of groups, the quasigroup that are not groups are more efficient and more secure than those based on

group. The result of the message would be more difficult to decode by unauthorized receiver.

As to claim 14, Seheidt et al. '173 as modified still does not teach wherein the encrypting is carried out using block ciphers.

Scheidt et al. '417, teaches cryptographic communication process and apparatus (see abstract), in which he teaches wherein the encrypting is carried out using block ciphers (see column 9, lines 23-25).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Seheidt et al. '173, as modified to include wherein the encrypting is carried out using block ciphers.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Seheidt et al. '173 as modified by the teaching of Scheidt et al. '417, because wherein the encrypting is carried out using block ciphers, would enable the cryptography method because; the security of the block cipher mode is based on the security of the text/key relation and the cryptanalytic resistant mixing properties of an iterated non-linear feedback function. The text/key relation is a symbol permutation consisting of the product of N randomly selected permutations, which are selected from a set of M permutations, which in turn are selected from the full set of W! permutations on W elements. The N permutations change according to a deterministic, but unknown, rule with each application of the function. Thus, even if the same symbol were presented to the text/key relation at two different

rounds within the processing of a single block, the permutation applied to that symbol would be the same only with a probability of 1/W. This maximizes the uncertainty across the total number of rounds of the block cipher (see Scheidt et al. '417, column 9, lines 28-42).

As to claim 15, Seheidt et al. '173 as modified teaches wherein the block cipher are defined by a function (see Scheidt et al. '417, column 9, lines 28-31).

As to claim 16, Seheidt et al. '173 as modified teaches wherein the block ciphers are formed using cross inversed quasigroups, used according to C =f *(M, K)* for the encryption and M=finv *(C,K)* for the decryption (see Scheidt et al. '417, column 8, lines 50-56; column 9, lines 16-27).

6. Claims 10 and 12-13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Seheidt et al. (U.S. patent 5,787,173) in view of Masters (U.S. patent 5,812,072) as applied in claims 1, 3-6, 9, 11, 19, 21-22, 29, and 31-32 above, and further in view of Hellman et al. (U.S. patent 4,424,414).

As to claim 10, Seheidt et al. as modified still, does not teach wherein the quasigroup is formed by an n by n square, where n is greater than 10^{10}.

Hellman et al., teaches exponentiation cryptographic apparatus and method (see abstract), in which he teaches wherein the quasigroup is formed by an n by n square, where n is greater than 10^{10} (see column 6, lines 19-24).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Seheidt et al., as modified, to include wherein the quasigroup is formed by an n by n square, where n is greater than 10^{10}.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Seheidt et al. as modified, by the teaching of Hellman et al., because wherein the quasigroup is formed by an n by n square, where n is greater than 10^{10}, would enable the cryptography method because the quasigroup is a set of objects with a multiplication table described by a latin square of size n x n and if n is smallest of 10^{10} the radio of the quasigroup will be infinity.

As to claim 12, Seheidt et al. as modified still does not teach wherein the first interiation is carried out in a different direction than the first encryption.

Hellman et al., teaches exponentiation cryptographic apparatus and method (see abstract), in which he teaches wherein the first interiation is carried out in a different direction than the first encryption (see column 4, lines 53-64).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Seheidt et al., as modified to include wherein the first interiation is carried out in a different direction than the first encryption.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Seheidt et al. as modified by

the teaching of Hellman et al., because wherein the first interiation is carried out in a different direction than the first encryption, would enable the cryptography method to make on the second encryption, the inverse- quasigroup.

As to claim 13, Seheidt et al. as modified teaches wherein the first direction is left to right and the second direction is right to left (see Hellman et al., column 4, lines 62-64).

7. Claims 23-26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Seheidt et al. (U.S. patent 5,787,173) in view of Anshel et al. (U.S. patent 5,440,640).

As to claim 23, Seheidt et al. teaches a cryptography method comprising encrypting information using an arithmetic with an algebraic structure (see column 4, lines 55-67).

Seheidt et al. does not teach the algebraic structure being a nongroup, nonfield structure.

Anshel et al., teaches multistream encryption system for secure communication (see abstract), in which he teaches the algebraic structure being a nongroup, nonfield structure (see abstract).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Seheidt et al., to include the algebraic structure being a nongroup, nonfield structure.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Seheidt et al. by the teaching of Anshel et al., because the algebraic structure being a nongroup, nonfield structure, would enable the cryptography method because the basic of encrypting require a non group algorithm, because is used has a key for encrypt the message.

As to claim 24, Seheidt et al. as modified teaches wherein the algebraic structure is not associative (see Seheidt et al., column 4, lines 57-60).

As to claim 25, Seheidt et al. as modified teaches wherein the algebraic structure is not commutative (see Seheidt et al., column 4, lines 57-60).

As to claim 26, Seheidt et al. as modified teaches the algebraic structure is not commutative (see Seheidt et al., column 4, lines 57-60).

8. Claim 33 is rejected under 35 U.S.C. 103(a) as being unpatentable over Seheidt et al. (U.S. patent 5,787,173) in view of Masters (U.S. patent 5,812,072) as applied in claims 1, 3-6, 9, 11, 19, 21-22, 29, and 31-32 above, and further in view of Hellman et al. (U.S. patent 4,218,582).

As to claim 33, Seheidt et al. as modified, does not teach an apparatus

further comprising using an additional encryption to provide an effective key size of x^2 of the original encryption.

Hellman et al., teaches exponentiation cryptographic apparatus and method (see abstract), in which he teaches an apparatus further comprising using an additional encryption to provide an effective key size of x^2 of the original encryption (see column 10, lines 61-64).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Seheidt et al. '17, as modified, to include an apparatus further comprising using an additional encryption to provide an effective key size of x^2 of the original encryption.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Seheidt et al. as modified, by the teaching of Hellman et al., because an apparatus further comprising using an additional encryption to provide an effective key size of x^2 of the original encryption, would enable the method to have space to the second encryption because is n x n (latin square) that duplicate the number.

Response to Arguments

9. Applicant's arguments filed 15-Mach-2005 with respect to the rejected claims in view of the cited references have been fully considered but they are not found persuasive:

In response to applicants' arguments that Scheidt "does not teach using a nontrivial CI quasigroup to encode the information", the arguments have been fully

considered but are not deemed persuasive, because Masters teaches encryption and decryption using arithmetic methods, (see Masters, column 3, lines 3-67).

"Transform a to a' where a' is the ordinal position of a in the sequence of integers prime to d.

Set b'=a'+d.

The transform is invertible as d can be recovered from a', b' and the a'.sup.th integer prime to d is readily computed as follows. Given a and d, a' is computed from a vector g.sub.1 . . . g.sub.r where g.sub.i is a prime dividing d", (see Masters, column 18, lines 15-30).

"The knowledge required for decoding can be considered as the key for an encrypted message", (see Masters, column 22, lines 30-39).

"It is here proposed to seek the representation of the non commutative properties of concatenation of uninterpreted symbols with objects derived from the commutative number systems. The strategy is to exploit the fact that the semigroup of endomorphisms of the direct product of commutative semigroups under composition is not in general commutative", (see Masters, column 34, lines 4-10).

Conclusion

10. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL.** See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

11. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Belix M. Ortiz whose telephone number is 571-272-4081. The examiner can normally be reached on moday-friday 9am-5pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Dov Popovici can be reached on 571-272-4083. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

bmo

May 25, 2005

SAM RIMELL
PRIMARY EXAMINER